(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（A）　(11)特許出願公開番号

特開平10－145773

(43)公開日　平成10年(1998)５月29日

(51)Int.Cl.[8]		識別記号	FI		
H04N	7/167		H04N	7/167	Z
G06F	12/14	320	G06F	12/14	320B
G09C	1/00	660	G09C	1/00	660Z
	5/00			5/00	
H04L	9/16		H04L	9/00	643

審査請求　未請求　請求項の数７　ＯＬ　（全８頁）

(21)出願番号　特願平8－302986

(22)出願日　平成８年(1996)11月14日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　石橋　泰博
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

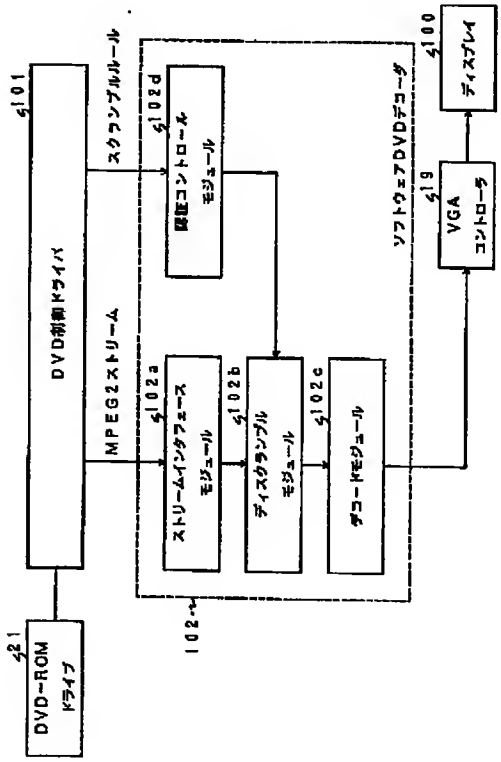
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　動画像データの暗号化方法およびその方法が適用されるコンピュータシステム並びに動画像データ符号化／復号化装置

(57)【要約】

【課題】動画データすべてを暗号化することなく、動画データの不正使用を防止する。

【解決手段】ＭＰＥＧ２データストリームに含まれるＩピクチャ、Ｐピクチャ、Ｂピクチャの中でＩピクチャに対してのみスクランブル処理などによる暗号化が施されており、ソフトウェアＤＶＤデコーダ１０２は、そのティスクランブルモジュール１０２ｄによってＩピクチャに対してのみディスクランブル処理を行う。これにより、ディスクランブル処理のために要するＣＰＵパワーを少なく抑制することが可能となり、動画データの復号処理をソフトウェアデコーダ１０２によってリアルタイムに行うことが可能となる。



【特許請求の範囲】
【請求項１】　フレーム内符号化画像およびフレーム間予測符号化画像を含むデジタル圧縮符号化された動画データに対して暗号化処理を施して、その動画データの不正使用を防止する動画像データ暗号化方法において、
前記デジタル圧縮符号化された動画データの中で前記フレーム内符号化画像に対してのみ暗号化処理を施し、
前記動画データの一部についてのみの暗号化によって動画データの不正な表示再生を防止できるようにしたことを特徴とする動画像データの暗号化方法。
【請求項２】　前記フレーム内符号化画像に対する暗号化処理は、前記フレーム内符号化画像を所定のルールで演算するスクランブル処理によって実行されることを特徴とする請求項１記載の暗号化方法。
【請求項３】　前記スクランブル処理されたフレーム内符号化画像を含む動画像データは、リードインエリア、プログラムエリア、およびリードアウトエリアから構成されるデータ列のプログラムエリアとして光ディスクに蓄積され、
前記リードインエリアには、
前記スクランブル処理のための演算ルールを示すスクランブルルール情報が格納されており、
前記光ディスクから前記プログラムエリアの動画データを読み出し、
その動画データに含まれるフレーム内符号化画像に対してその逆スクランブルのための演算処理を前記スクランブルルール情報に基づいて実行した後、動画データの復号を行うことを特徴とする請求項２記載の暗号化方法。
【請求項４】　前記動画データのデータ列は、ヘッダ部とデータ部とから構成されており、
前記ヘッダ部には、
前記暗号化処理されたフレーム内符号化画像の位置を示す情報が含まれていることを特徴とする請求項１記載の暗号化方法。
【請求項５】　動画像をデジタル圧縮符号化し、フレーム内符号化画像およびフレーム間予測符号化画像を生成する動画像符号化手段と、
この動画像符号化手段で符号化されたフレーム内符号化画像に対して暗号化処理を施す手段とを具備し、
前記動画データの一部についてのみの暗号化によって動画データの不正使用を防止できるようにしたことを特徴とする動画像符号化装置。
【請求項６】　フレーム内符号化画像およびフレーム間予測符号化画像を含むデジタル圧縮符号化された動画像データを復号する動画像復号装置において、
前記デジタル圧縮符号化された動画像データから暗号化処理されたフレーム内符号化画像を抽出し、その暗号化されたフレーム内符号化画像を解読する手段を具備することを特徴とする動画像復号化装置。
【請求項７】　ＣＰＵと、デジタル圧縮符号化された動画データが蓄積された蓄積メディアからデータを読み出すためのディスクドライブ装置を制御可能なディスクインターフェースとを備え、前記デジタル圧縮符号化された動画データの復号及び再生が可能なコンピュータシステムにおいて、
前記ＣＰＵに、前記ディスクインターフェースを介して前記ディスクドライブ装置から読み出される動画データの中から暗号化処理されたフレーム内符号化画像を抽出させる手段と、
前記ＣＰＵに、その抽出されたフレーム内符号化画像の解読処理を実行させる手段とを具備することを特徴とするコンピュータシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は動画像データの暗号化方法およびその方法が適用されるコンピュータシステム並びに動画像データ符号化／復号化装置に関する。
【０００２】
【従来の技術】近年、コンピュータ技術の発達に伴い、いわゆるマルチメディア対応のパーソナルコンピュータが種々開発されている。この種のパーソナルコンピュータでは、テキストデータやグラフィックスデータの他に、動画や音声データを再生することができる。
【０００３】通常、動画データはＭＰＥＧ１によって圧縮符号化されてＣＤ（Ｃｏｍｐａｃｔ　Ｄｉｓｋ）などに記憶されており、その動画データのデコードおよび表示再生には、専用の拡張ボードが使用されている。動画データのデコードおよび表示再生を行う拡張ボードとしては、例えば、米シグマデザイン社の“ＲＥＡＬ　Ｍａｇｉｃ”が良く知られている。この“ＲＥＡＬ　Ｍａｇｉｃ”は、ＭＰＥＧ１の規格に準拠したビデオデコード機能を有しており、デコードされた動画データは、フィーチャコネクタを介してビデオカードから取り込まれたＶＧＡグラフィクスと合成されて表示される。
【０００４】しかし、ＭＰＥＧ１の規格は、１．５Ｍｂｐｓ程度のデータ転送速度を持つＣＤを使用することを前提とした規格であり、映画などの大量の画像情報を含む動画データを扱うと、画質の劣化などの問題が生じる。
【０００５】そこで、最近では、ＣＤの数倍乃至十数倍程度のデータ転送速度を持つ新世代の蓄積メディアとしてＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋ）が開発されている。ＤＶＤはＭＰＥＧ２という動画像符号化を使って、ＣＤと同じ大きさの光ディスクに、映画などの映像情報を高画質で記録できる新しいビデオディスク規格である。ＤＶＤの記録再生方法は、画質と、容量に対する記録時間の双方を確保する観点から、可変レート符号化の考えに基づいている。可変レート符号化データのデータ量は、元の画像の画質に依存し、動きの激しいシーンほどそのデータ量は増加する。

【０００６】このＤＶＤに蓄積された動画データをパーソナルコンピュータ上で再生する場合には、ＤＶＤ－ＲＯＭからコンピュータの主記憶にデータが読み込まれ、そしてそれがＤＶＤデコーダに転送されることになる。この場合、主記憶に読み込まれたデータの不正コピー、およびその不正使用を防止するためには、動画データに含まれるすべての映像情報に対してスクランブル処理などの暗号化を施すことが必要となる。

【０００７】ところで、近年のＣＰＵの高速化により、専用のハードウェアによって動画データをデコードするのではなく、ソフトウェアによって動画データをデコードするという、いわゆるソフトウェアデコーダの実現が望まれている。ソフトウェアデコーダによって動画データをデコードすることにより、専用のハードウェアが不要となり、システム全体のコストを低減することが可能となる。

【０００８】しかし、ソフトウェアデコーダを使用した場合には、ＭＰＥＧ２で符号化された動画データを復号するという本来の処理のみならず、それに先だって、スクランブル処理された動画データを元に戻すというディスクランブル処理についてもＣＰＵによって実行することが必要とされる。ディスクランブル処理の対象となるのは動画データに含まれるすべての映像情報であるため、それに要するＣＰＵの負荷はかなり大きい。従って、ＣＰＵパワーの多くがディスクランブル処理に取られてしまい、リアルタイムにデコード処理を行うことは実際上困難である。

【０００９】

【発明が解決しようとする課題】上述したように、従来では、映像情報すべてをスクランブルしているため、そのディスクランブル処理のために多くのＣＰＵパワーが必要とされる。したがって、コピープロテクト機能とソフトウェアデコーダとを同時に満足することは実際上困難であった。

【００１０】この発明はこのような点に鑑みてなされたものであり、動画データの一部のみを暗号化するだけでその動画データの表示再生などの不正使用を防止できるようにし、コピープロテクト機能とソフトウェアデコーダとを同時に満足させることが可能な動画像データの暗号化方法およびその方法が適用されるコンピュータシステム並びに動画像データ符号化／復号化装置を提供することを目的とする。

【００１１】

【課題を解決するための手段】この発明は、フレーム内符号化画像およびフレーム間予測符号化画像を含むデジタル圧縮符号化された動画データに対して暗号化処理を施して、その動画データの不正使用を防止する動画像データ暗号化方法において、前記デジタル圧縮符号化された動画データの中で前記フレーム内符号化画像に対してのみ暗号化処理を施し、前記動画データの一部についてのみの暗号化によって動画データの不正な表示再生を防止できるようにしたことを特徴とする。

【００１２】この動画像データ暗号化方法においては、ＭＰＥＧ２などでデジタル圧縮符号化された動画データにおいては、フレーム内符号化画像（Ｉピクチャ）、片方向予測、双方向予測などのフレーム間予測符号化画像（Ｐピクチャ、Ｂピクチャ）が含まれているが、フレーム間予測符号化画像（Ｐピクチャ、Ｂピクチャ）の復号は、フレーム内符号化画像（Ｉピクチャ）を用いて行われており、フレーム内符号化画像（Ｉピクチャ）無しではフレーム間予測符号化画像（Ｐピクチャ、Ｂピクチャ）を正しく復号することができない点に着目し、フレーム内符号化画像（Ｉピクチャ）に対してのみスクランブル処理などによる暗号化を施したものである。

【００１３】これにより、動画データに含まれるすべての画像情報に対してスクランブル処理を行うのではなく、動画データの一部についてのみのスクランブル処理で不正な表示再生を防止できるようになる。従って、ソフトウェアデコーダを利用する場合には、ディスクランブル処理のために要するＣＰＵパワーを少なく抑制することが可能となり、動画データの復号処理をソフトウェアデコーダによってリアルタイムに行うことが可能となる。

【００１４】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。図１には、この発明の一実施形態に係るコンピュータシステムで使用されるソフトウェアデコーダとその周辺のソフトウェア及びハードウェアの構成が示されている。ＤＶＤ－ＲＯＭドライブ２１は光ディスクから構成されるＤＶＤメディアに蓄積されたビデオ、オーディオ、サブピクチャを含むＭＰＥＧ２データストリームを読み出すためのものであり、ＤＶＤメディアに蓄積された動画データのストリームは図２のようなデータフォーマットを有している。

【００１５】すなわち、データストリームは複数のセクタから構成されているが、動画データについては、各セクタは、図示のようにストリームヘッダ部とＭＰＥＧ２データ部とから構成されている。ＭＰＥＧ２データ部には、ＭＰＥＧ２でデジタル圧縮符号化された画像、つまりＩピクチャ、Ｐピクチャ、Ｂピクチャが含まれている。このうち、Ｉピクチャについてはその画像に対して所定の演算ルールでスクランブル処理が施されており、他のＰピクチャ、Ｂピクチャについてはそのようなスクランブル処理は施されてない。ストリームヘッダ部には、スクランブル処理されている画像データの位置、つまりＩピクチャの位置を示すスクランブル情報が含まれている。スクランブル情報については、暗号化処理を施しておいてもよい。このようなデータフォーマットでＭＰＥＧ２データストリームを生成する符号化装置は、図４のように構成されている。

【００１６】すなわち、図４に示されているように、符号化装置は、映画の主映像に相当するビデオデータをＭＰＥＧ２でデジタル圧縮符号化するＭＰＥＧ２エンコーダ５０１、オーディオ信号をドルビーＡＣ３でデジタル圧縮符号化するオーディオエンコーダ５０２、および字幕などのサブピクチャをランレングス符号化などでデジタル圧縮符号化するサブピクチャエンコーダ５０３を備えている。ＭＰＥＧ２エンコーダ５０１で符号化されたビデオデータには、前述のＩピクチャ、Ｐピクチャ、Ｂピクチャが含まれているが、ＩピクチャについてはＩピクチャスクランブラ５０４によってビデオデータの中から抽出されてスクランブル処理が施される。そして、多重化回路５０５において、符号化されたビデオデータ、オーディオデータ、サブピクチャデータが一本のＭＰＥＧ２プログラムストリームとして多重化されて、ＤＶＤメディアに蓄積される。

【００１７】図１のＤＶＤ制御ドライバ１０１はＤＶＤ－ＲＯＭドライブ２１からのＭＰＥＧ２データの読み出しを制御するソフトウェアであり、動画再生時にＭＰＥＧ２データをＤＶＤ－ＲＯＭドライブ２１から読み出し、ソフトウェアＤＶＤデコーダ１０２に渡す。このＤＶＤ制御ドライバ１０１はＯＳの一部として実現することもできる。

【００１８】ソフトウェアＤＶＤデコーダ１０２は、ＤＶＤメディアに蓄積されているＭＰＥＧ２データを復号するためのものであり、図示のように、ストリームインタフェースモジュール１０２ａ、ディスクランブルモジュール１０２ｂ、デコードモジュール１０２ｃ、および認証モジュール１０２ｄから構成されている。ストリームインタフェースモジュール１０２ａは、ＤＶＤ制御ドライバ１０１を介して図２で説明したＭＰＥＧ２データ部とスクランブル情報をＤＶＤ－ＲＯＭドライブ２１から取得し、それをディスクランブルモジュール１０２ｂに渡す。

【００１９】認証コントロールモジュール１０２ｄは、ＤＶＤ制御ドライバ１０１を介してあるいは直接にＤＶＤ－ＲＯＭドライブ装置２１と通信し、正当なソフトウェアモジュールであることをＤＶＤ－ＲＯＭドライブ装置２１に通知するという認証処理を行う。そして、正当なソフトウェアモジュールであることが承認されると、ＤＶＤ－ＲＯＭドライブ装置２１からのスクランブルルール情報の読み出しが許可される。このスクランブルルール情報はＩピクチャに対して施されたスクランブル処理の演算ルールを示すものであり、このスクランブルルール情報に対しても所定の暗号化処理が施されている。認証コントロールモジュール１０２ｄはスクランブルルール情報を解読し、それをディスクランブルモジュール１０２ｂに渡す。

【００２０】スクランブルルール情報は、ＤＶＤメディアの最内周から最外周に渡る一本のデータ列の中で通常のファイルシステムなどからはその読み出しができない位置、つまりリードインエリアに格納しておくことが好ましい。すなわち、光ディスクなどの蓄積媒体におけるデータ格納形式では、データは、図３に示されているようにリードインエリア、データエリア、リードアウトエリアから構成されているが、リードインエリアの内容は通常のファイルシステムから参照することはできない。このため、スクランブルルール情報をリードインエリアに格納しておくことにより、スクランブルルール情報が盗み見られることを防止することができる。

【００２１】ディスクランブルモジュール１０２ｂは、ＭＰＥＧ２データ部に含まれるＩピクチャの位置をスクランブル情報に基づいて特定し、ＭＰＥＧ２データ部からＩピクチャを抽出する。そして、認証コントロールモジュール１０２ｄから得たスクランブルルール情報に基づいて、スクランブルされているＩピクチャを元に戻すディスクランブル処理のための演算を実行する。

【００２２】デコードモジュール１０２ｃは、ＭＰＥＧ２データを復号してそれを圧縮前の元の情報に伸張するものであり、ビデオデータのデコードだけでなく、サブピクチャおよびオーディオのデコードも行う。デコードされたビデオデータはデコードされたサブピクチャと合成されてＶＧＡコントローラ１９に送られ、ディスプレイ１００に画面表示される。また、デコードされたオーディオデータはオーディオコントローラによって再生される。

【００２３】次に、図５のフローチャートを参照して、動画再生処理の手順を説明する。動画データ再生用のアプリケーションプログラムから動画データの再生要求が発行されると、まず、認証コントロールモジュール１０２ｄがＤＶＤ－ＲＯＭドライブ２１と通信してスクランブルルールを取得し、それを解読する（ステップＳ１０１）。次いで、ストリームインタフェースモジュール１０２ａがＭＰＥＧ２ストリームを取得し、スクランブル情報とＭＰＥＧ２データをディスクランブルモジュールに渡す（ステップＳ１０２）。この時、必要に応じてスクランブル情報の解読も行われる（ステップＳ１０３）。スクランブル情報の解読はディスクランブルモジュール１０２ｂで行うことも可能である。

【００２４】この後、ディスクランブルモジュール１０２ｂがＭＰＥＧ２データに含まれるＩピクチャの位置をスクランブル情報に基づいて特定し、認証コントロールモジュール１０２ｄから得たスクランブルルール情報に基づいてスクランブルされているＩピクチャを元に戻すディスクランブル処理を実行する（ステップＳ１０４）。そして、デコードモジュール１０２ｃによってＭＰＥＧ２データが復号がされ、動画及び音声の再生が行われる（ステップＳ１０５）。

【００２５】以上のように、この実施形態においては、ＭＰＥＧ２データストリームにはフレーム内符号化され

たＩピクチャ、片方向予測、双方向予測のフレーム間予測符号化されたＰピクチャ、Ｂピクチャが含まれているが、Ｐピクチャ、Ｂピクチャの復号は、Ｉピクチャを用いて行われており、Ｉピクチャ無しではＰピクチャ、Ｂピクチャを正しく復号することができない点に着目し、Ｉピクチャに対してのみスクランブル処理などによる暗号化を施している。これにより、すべての画像情報に対してスクランブル処理を行うのではなく、動画データの一部についてのみのスクランブル処理で不正な表示再生を防止できるようになる。従って、ディスクランブル処理のために要するＣＰＵパワーを少なく抑制することが可能となり、動画データの復号処理をソフトウェアデコーダ１０２によってリアルタイムに行うことが可能となる。

【００２６】また、専用のハードウェアデコーダを有するコンピュータシステムでは、ディスクランブル処理とデコード処理をハードウェアデコーダによって実行させることもできる。この場合、ディスクランブル処理はＩピクチャに対してだけ行えばよいので、ディスクランブル処理のための回路は簡単に構成できる。このような専用のハードウェアデコーダを有するコンピュータシステムの構成例を図６に示す。

【００２７】このシステムはデスクトップ型パーソナルコンピュータに対応するものであり、図示のように、ＰＣＩバス１０、ＣＰＵ１１、主メモリ（ＭＥＭ）１２、ＨＤＤ１３、ＡＴＡＰＩまたはＳＣＳＩインタフェースから構成されるＤＶＤインターフェース１６、オーディオコントローラ１７、ＤＶＤデコーダ１８、マルチメディアディスプレイコントローラ１９、およびビデオメモリ（ＶＲＡＭ）２０を備えており、ＭＰＥＧ２によって符号化された動画データなどを格納したＤＶＤ－ＲＯＭドライブ２１は、ＤＶＤインターフェース１６に接続されている。

【００２８】ＣＰＵ１１は、このシステム全体の動作を制御するものであり、システムメモリ（ＭＥＭ）１２に格納されたオペレーティングシステムおよび実行対象のアプリケーションプログラムを実行する。ＤＶＤ－ＲＯＭドライブ２１に記録されたデータの転送及び再生は、ＣＰＵ１１にＤＶＤ制御ドライバを実行させることによって実行される。

【００２９】ＤＶＤインタフェース１６は、ＨＤＤやＣＤ－ＲＯＭなどのディスク装置装置をＰＣＩバス１０に接続するためのディスクインタフェースであり、この実施形態では、ＣＰＵ１１からの指示に従いＤＶＤ－ＲＯＭドライブ２１との間のデータ転送を行う。オーディオコントローラ１７は、ＣＰＵ１１の制御の下にサウンドデータの入出力制御を行うものであり、サウンド出力のために、ＰＣＭ音源１７１、ＦＭ音源１７２、マルチプレクサ１７３、およびＤ／Ａコンバータ１７４を備えている。マルチプレクサ１７３には、ＰＣＭ音源１７１およびＦＭ音源１７２からの出力と、ＤＶＤデコーダ１８から転送されるデジタルオーディオデータが入力され、それらの１つが選択される。

【００３０】デジタルオーディオデータは、ＤＶＤ－ＲＯＭドライブ２１から読み出されたオーディオデータをデコードしたものである。ＤＶＤデコーダ１８からオーディオコントローラ１７へのデジタルオーディオデータの転送には、オーディオバス１８ａが用いられ、ＰＣＩバス１０は使用されない。従って、コンピュータシステムの性能に影響を与えることなくデジタルオーディオデータの高速転送が可能となる。

【００３１】ＤＶＤデコーダ１８は、ＣＰＵ１１の制御の下に、ＤＶＤインターフェース１６からＭＰＥＧ２プログラムストリームを読み出し、それをビデオ、サブピクチャ、およびオーディオパケットに分離した後、それらをそれぞれデコード処理し同期化して出力する。このＤＶＤデコーダ１８は、例えばこのコンピュータシステムのＰＣＩ拡張スロットに取り外し自在に装着できるＰＣＩ拡張カードとして実現されており、図示のように、マスタトランザクション制御部２０１、ディスクランブル制御部２０２、ＭＰＥＧ２デコーダ２０３が設けられている。

【００３２】マスタトランザクション制御部２０１は、ＤＶＤデコーダ１８をＰＣＩバス１０上にトランザクションを発行するバスマスタ（イニシエータ）として動作させるためのものであり、ＤＶＤインターフェース１６から動画データを読み出すためのＩ／Ｏリードトランザクションを実行する。マスタトランザクション制御部２０１によって読みとられたＭＰＥＧ２プログラムストリームは、ディスクランブル制御部２０２でＩピクチャについてのディスクランブルが行われた後、ＭＰＥＧ２デコーダ２０３に送られる。ＭＰＥＧ２デコーダ２０３では、ＭＰＥＧ２プログラムストリームからビデオ、サブピクチャ、およびオーディオパケットへの分離処理と、それらのデコード処理が行われる。

【００３３】デコードされたオーディオデータは、前述したようにデジタルオーディオデータとしてオーディオバス１８ａを介してオーディオコントローラ１８ａに転送される。デコードされたビデオおよびサブピクチャは合成されて、デジタルＹＵＶデータとしてマルチメディアディスプレイコントローラ１９に送られる。この場合、ＤＶＤデコーダ１８からマルチメディアディスプレイコントローラ１９へのデジタルＹＵＶデータの転送には、ビデオバス１８ｂが用いられ、ＰＣＩバス１０は使用されない。従って、デジタルＹＵＶデータの転送についても、デジタルオーディオデータと同様に、コンピュータシステムの性能に影響を与えることなく高速に行うことができる。

【００３４】ビデオバス１８ｂとしては、ＶＥＳＡ規格のＶＡＦＣ（ＶＥＳＡ Ａｄｖａｎｃｅｄ Ｆｅａｔｕ

ｒｅ　Ｃｏｎｎｅｃｔｏｒ）、またはVM－Ｃｈａｎｎｅｌ（VESA Ｍｅｄｉａ　Ｃｈａｎｎｅｌ）を利用することができる。

【００３５】また、ＤＶＤデコーダ１８は、デジタルＹＵＶデータとオーディオデータをＮＴＳＣ方式のＴＶ信号に変換してＴＶ受像機の外部ビデオ入力に出力する機能も有している。ＤＶＤデコーダ１８からＴＶ受像機へのＴＶ信号の送信は、ＤＶＤデコーダ１８のカードに設けられたコネクタに、ＴＶ受像機への導出ケーブルを接続することによって容易に行うことができる。

【００３６】マルチメディアディスプレイコントローラ１９は、ＣＰＵ１１の制御の下に、このシステムのディスプレイモニタとして使用されるＣＲＴディスプレイを制御するものであり、ＶＧＡ仕様のテキストおよびグラフィクス表示の他、動画表示をサポートする。

【００３７】このマルチメディアディスプレイコントローラ１９には、図示のように、グラフィックス表示制御回路（Graphics）１９１、ビデオ表示制御回路１９２、マルチプレクサ１９３、およびＤ／Ａコンバータ１９４等が設けられている。

【００３８】グラフィックス表示制御回路１９１は、ＶＧＡ互換のグラフィックスコントローラであり、ビデオメモリ（ＶＲＡＭ）２０に描画されたＶＧＡのグラフィクスデータをＲＧＢビデオデータに変換して出力する。ビデオ表示制御回路１９２は、デジタルＹＵＶデータを貯えるビデオバッファ、及び同バッファに貯えられたＹＵＢデータをＲＧＢビデオデータに変換するＹＵＢ－ＲＧＢ変換回路等をもつ。

【００３９】マルチプレクサ１９３は、グラフィックス表示制御回路１９１とビデオ表示制御回路１９２の出力データの一方を選択、またはグラフィックス表示制御回路１９１からのＶＧＡグラフィクス上にビデオ表示制御回路１９２からのビデオ出力を合成してＤ／Ａコンバータ１９４に送る。Ｄ／Ａコンバータ１９４は、マルチプレクサ１９４からのビデオデータをアナログＲＧＢ信号に変換して、ＣＲＴディスプレイに出力する。

【００４０】

【発明の効果】以上説明したように、この発明によれば、動画データの一部のみを暗号化するだけでその動画データの表示再生などの不正使用を防止できるようになり、コピープロテクト機能とソフトウェアデコーダとを同時に満足させることが可能となる。

【図面の簡単な説明】

【図１】この発明の一実施形態に係るコンピュータシステムで使用されるソフトウェアデコーダの機能構成を示すブロック図。

【図２】同実施形態で使用される動画データストリームのデータ構造を示す図。

【図３】同実施形態で使用されるスクランブルルール情報の格納位置を示す図。

【図４】同実施形態で使用される符号化装置の構成を示すブロック図。

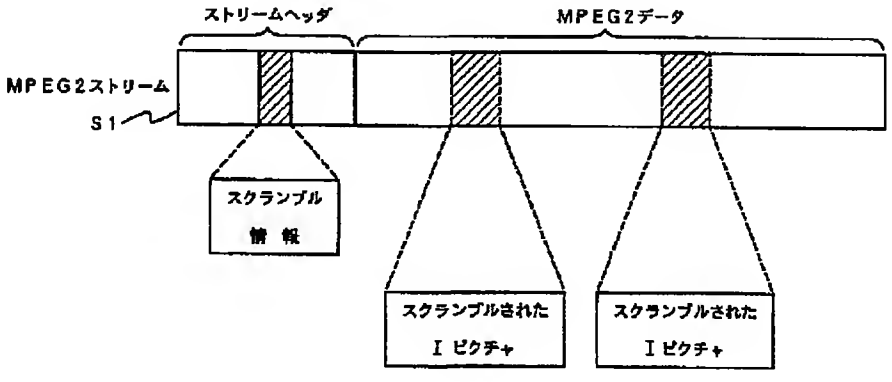
【図５】同実施形態における動画再生処理の手順を示すフローチャート。

【図６】同実施形態のシステムのハードウェア構成を示すブロック図。

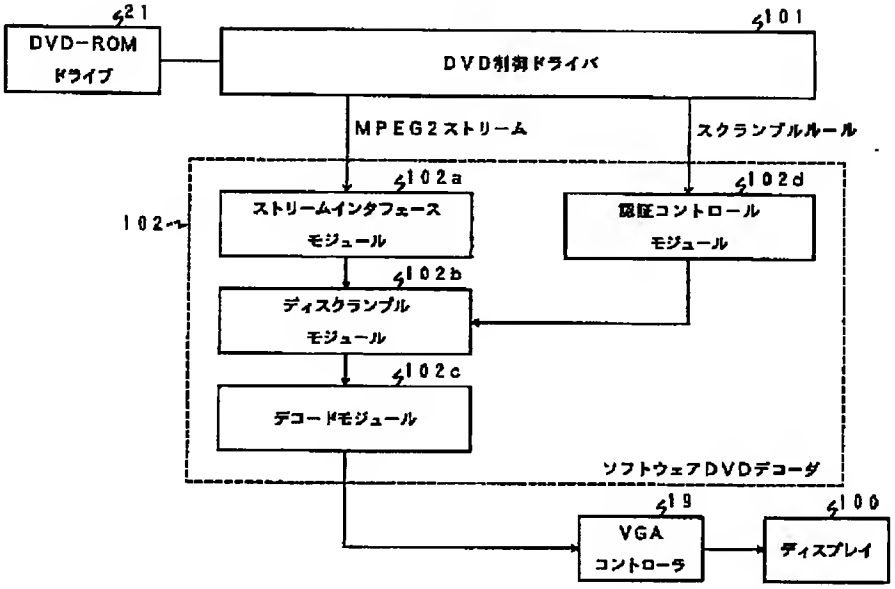
【符号の説明】

１０１…ＤＶＤ制御ドライバ、１０２…ソフトウェアＤＶＤデコーダ、１０２ａ…ストリームインタフェースモジュール、１０２ｂ…ディスクランブルモジュール、１０２ｃ…デコードモジュール、１０２ｄ…認証モジュール、１０…システムバス、１１…ＣＰＵ、１２…システムメモリ、１６…ＡＴＡＰＩインタフェース、１７…オーディオコントローラ、１８…ＤＶＤデコーダ、１９…マルチメディアディスプレイコントローラ、２０…ビデオメモリ、２１…ＤＶＤ－ＲＯＭドライブ、１６１…Ｉ／Ｏポート、２０１…マスタトランザクション制御部、２０２…ディスクランブル制御部、２０３…ＭＰＥＧ２デコーダ。

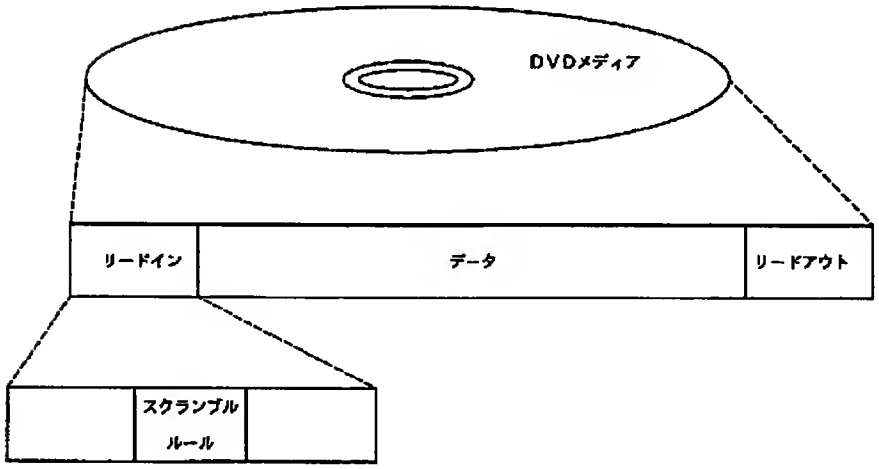
【図２】



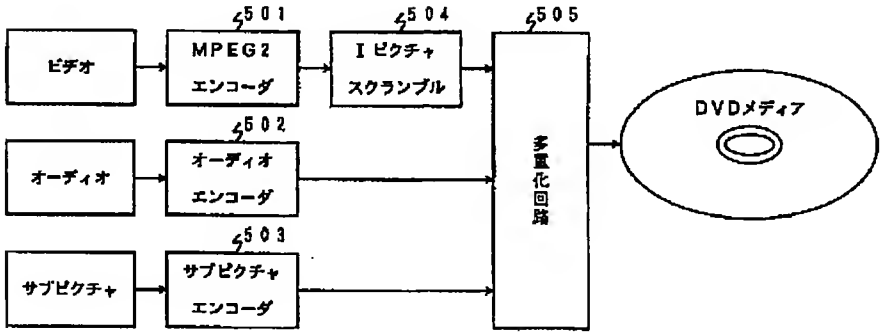
【図１】


21
DVD-ROM
ドライブ
101
DVD制御ドライバ
MPEG2ストリーム
スクランブルルール
102a
ストリームインタフェース
モジュール
102d
認証コントロール
モジュール
102
102b
ディスクランブル
モジュール
102c
デコードモジュール
ソフトウェアDVDデコーダ
19
VGA
コントローラ
100
ディスプレイ

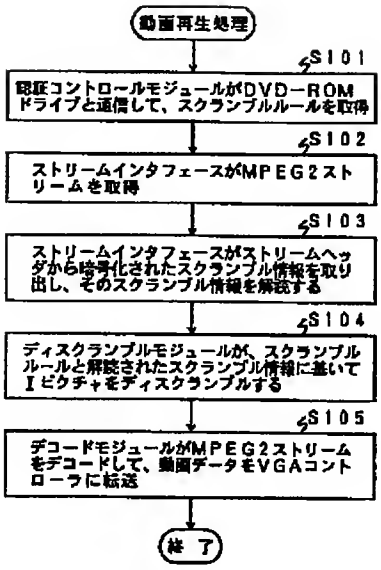
【図３】


DVDメディア
リードイン
データ
リードアウト
スクランブル
ルール

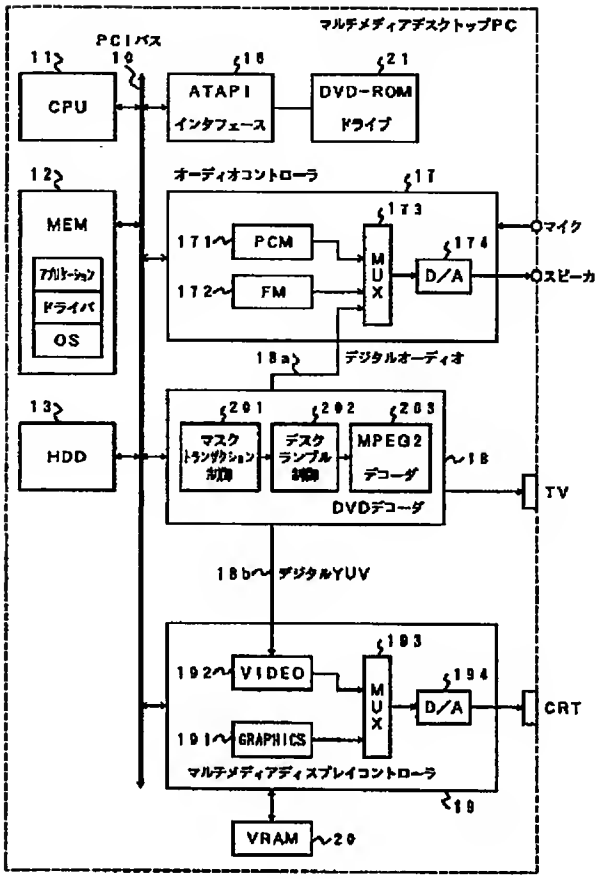
【図４】


ビデオ
501
MPEG2
エンコーダ
504
Iピクチャ
スクランブル
505
オーディオ
502
オーディオ
エンコーダ
サブピクチャ
503
サブピクチャ
エンコーダ
多重化回路
DVDメディア

【図５】


動画再生処理
S101
認証コントロールモジュールがDVD-ROMドライブと通信して、スクランブルルールを取得
S102
ストリームインタフェースがMPEG2ストリームを取得
S103
ストリームインタフェースがストリームヘッダから暗号化されたスクランブル情報を取り出し、そのスクランブル情報を解読する
S104
ディスクランブルモジュールが、スクランブルルールと解読されたスクランブル情報に基いてIピクチャをディスクランブルする
S105
デコードモジュールがMPEG2ストリームをデコードして、動画データをVGAコントローラに転送
終了

【図６】


マルチメディアデスクトップPC
PCIバス
10
11
CPU
16
ATAPI
インタフェース
21
DVD-ROM
ドライブ
12
MEM
アプリケーション
ドライバ
OS
オーディオコントローラ
17
173
171
PCM
172
FM
MUX
174
D/A
マイク
スピーカ
18a
デジタルオーディオ
13
HDD
201
マスクトランザクション制御
202
デスクランブル制御
203
MPEG2
デコーダ
18
DVDデコーダ
TV
18b
デジタルYUV
193
192
VIDEO
194
D/A
CRT
191
GRAPHICS
マルチメディアディスプレイコントローラ
19
VRAM
20

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-342246
(P2004-342246A)
(43)公開日　平成16年12月2日(2004.12.2)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G11B 20/10	G11B 20/10	H	5B017
G06F 12/14	G06F 12/14	320B	5D044
G11B 20/12	G06F 12/14	320E	5D110
G11B 27/00	G06F 12/14	320F	5J104
H04L 9/08	G11B 20/12		

審査請求 未請求　請求項の数 28　OL　（全 46 頁）　最終頁に続く

(21)出願番号　特願2003-138551(P2003-138551)
(22)出願日　平成15年5月16日(2003.5.16)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(72)発明者　木谷　聡
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、情報記録媒体、コンテンツ管理システム、および方法、並びにコンピュータ・プログラム

(57)【要約】
【課題】情報記録媒体に格納される暗号化コンテンツの不正利用の防止、不正複製についての情報漏えいルート解析を可能とした構成を提供する。
【解決手段】コンテンツ編集エンティテイが、記録シード（ＲＥＣ　ＳＥＥＤ）を生成し、管理センタから受領する鍵情報、および鍵生成情報（第２シード）に基づいて第２ブロックキーＫｂ２を生成し、第２ブロックキーＫｂ２に基づくコンテンツ暗号化を実行する。情報記録媒体製造エンティテイが、物理インデックスを生成し、管理センタから受領する鍵情報、および鍵生成情報（第１シード）に基づいてブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づく第２シードの暗号化を実行し、これらの情報および各エンティテイのコード情報を情報記録媒体に格納する。
【選択図】　図１８